ABSTRACT OF THE DISCLOSURE

A method and system for revoking a certificate issued by a certification authority (CA). An identifier associated with a registration authority (RA) that requested issuance of a certificate on behalf of a principal is included within the certificate that is issued by the CA. Additionally, a time stamp indicating when the respective RA requested the certificate may be included in the certificate. In response to a request from a principal to a server for access to a resource, the server verifies the request using a decryption key contained in the certificate. Additionally, in a first embodiment a determination is made whether the RA identifier contained within the certificate is present on a certificate revocation list (CRL) maintained by a revocation server. If the RA identifier is present on the CRL, an indication is provided to the server that the certificate has been revoked and access to the requested resource mayb be denied. In a second embodiment, a determination is made whether the RA identifier is contained on the CRL and whether the time stamp contained within the certificate corresponds to a time period indicated in the CRL during which the respective RA was deemed untrustworthy. If the RA identifier in the certificate corresponds to an RA identifier on the CRL and the time stamp in the certificate is within a period in which the respective RA was deemed untrustworthy, an indication is provided to the respective server that the

ATTORNEY DOCKET NO. P4098
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

certificate has been revoked and access to the requested resource may be denied.

238563

ATTORNEY DOCKET NO. P4098
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES LLP
TEL. (617) 542-2290
FAX. (617) 451-0313